TOP SECRET

SELECTED EXAMPLES OF POSSIBLE APPROACHES TO ELECTRONIC COMMUNICATION INTERCEPTION OPERATIONS

MITRE Technical Report

MTR-7461

SELECTED EXAMPLES

OF POSSIBLE APPROACHES

TO ELECTRONIC COMMUNICATION

INTERCEPTION OPERATIONS

C.W. SANDERS
G.F. SANDY
J.F. SAWYER

J A N U A R Y 1 9 7 7

CONTRACT SPONSOR Office of Telecommunications Policy
CONTRACT NO. TP6AC039
PROJECT NO. 2430
DEPT. W-33

THE MITRE CORPORATION
METREK DIVISION

MITRE Department
and Project Approval: Charles La Pedus

OFFICE OF TELECOMMUNICATIONS POLICY
EXECUTIVE OFFICE OF THE PRESIDENT
WASHINGTON, D.C. 20504

DIRECTOR

FOREWORD

Executive Order 11556 requires the Director, Office of Telecommunications Policy, to develop policies with respect to telecommunications that will promote the public interest and support the national security. Further, the Director is to formulate policies for Executive Branch telecommunications activities which include considerations of privacy, security and emergency readiness. These assignments have resulted over the past few years in research by the Office of Telecommunications Policy into questions of communications privacy which include the extent of privacy vulnerability in our nation's telecommunications systems, and the strengths and weaknesses of existing wiretapping and eavesdropping statutes.

Following an examination of the legal safeguards against electronic eavesdropping, performed by Professor Kent Greenawalt, the MITRE Corporation was commissioned in June 1976 to determine the extent to which various methods of electronic telecommunications are vulnerable to invasions of privacy by electronic interception. A thorough understanding of the technical vulnerability of electronic communications to interference and interception was deemed necessary to the development of more effective national safeguards. In addition, any judgment on our part regarding the efficacy of legal safeguards against privacy invasions must take into account the degree to which various methods of surreptitious interception of telecommunications were detectable.

The two-volume study of "Vulnerability of Electronic Communications Systems to Electronic Interception," dated January 1977 (Volume I-PB 264 447-and Volume II-PB 264 448-1), responded to these needs. They were received and released to the public through the National Technical Information Service in January 1977. The researchers developed "scenarios" of surreptitious interception as a research device which would make potential methods of electronic interception more easily identifiable for detailed technical examination. The contractor's working papers which contained the scenarios were later forwarded to this Office because Federal Procurement Regulations require that all working papers of the contractor belong to the contracting agency. Because of their explicit nature, these papers were not released as part of the study.

The reader should be aware that unauthorized interception of or the attempt to intercept wire communications is prohibited by federal law (18 USC 2510, 2511). Any person found to be in violation of this statute is subject to a $10,000 fine or imprisonment for five years or both. We have enclosed for your information a copy of the existing wiretap laws.

Sincerely,

William J. Thaler
Acting

ABSTRACT

This report presents three detailed examples of possible approaches to electronic interception of electronic communication systems. The examples illustrate strategies and techniques that could be employed in intercepting communications over both local loops and toll facilities.

TABLE OF CONTENTS

1.0 INTRODUCTION

This report outlines three examples of possible approaches to electronic communication interception. The purpose is to illustrate the types of strategies that could be employed in carrying out an electronic communications interception operation. This report assumes as background the materials presented in MTR-7439, Vulnerability of Electronic Communication Systems to Electronic Interception. Volume I of MTR-7439 presented a number of general strategies for intercepting communications carried by a variety of communication systems. Perforce the descriptions had to be rather abbreviated in order to cover the full range of strategies which might be employed by an interceptor. This volume outlines three specific interception strategies to provide a more detailed illustration of possible interceptor approaches. These are:

1. Interception of a suburban residential telephone.
2. Interception of a business's data communication to a computer service.
3. Interception of conversations over the direct distance dialing network between two specific individuals in different cities.

It is necessary to make specific assumptions about the objectives of the interceptor, the characteristics of the telephone company plant and the target and the environment within which the operation is to take place. These assumptions are stated for each case under the heading. "Situation".

2.0 INTERCEPTION OF A SUBURBAN RESIDENTIAL TELEPHONE

2.1 Situation

The interceptor is interested in conversations a particular individual might have with other unknown individuals. He would also like to know the identity of the other party to the conversation of interest, if possible. The information of interest would be communicated using the targeted individual's home telephone sometime between

6 PM and 11 PM, Monday through Friday. The call could be originated by the targeted individual or by one of the unknown individuals. The residential area is similar to that found in Northern Virginia outside the Beltway. The interceptor knows the location of the home of the targeted individual.

Since the interceptor does not know the identity of the other individuals, nor who will originate the call(s) of interest, he must perform his interception on the local subscriber loop.

The local subscriber loop consists of an aerial drop wire from the house to a nearby pole-mounted terminal where it is connected to an aerial distribution cable consisting of 25 pairs. The distribution cable runs several blocks to another pole-mounted terminal where it connects to an aerial branch feeder cable consisting of 200 pairs (made up of 8 binder groups). The branch feeder cable runs several blocks to another pole-mounted terminal where it connects with an aerial main feeder cable consisting of 600 pairs (made up of 24 binder groups). All cable except the drop wire is Alpeth (consisting of a polyethylene and aluminum sheath). The main branch feeder cable is pressurized. None of the terminal cases or other terminal appearances are locked or pressurized. Initially unknown to the interceptor, the only suitable place to hide his monitoring station is a wooded section adjacent to a section of the main feeder cable.

2.2 Signal Acquisition Strategy

A possible strategy for the interceptor is as follows:

1. Visually trace drop wire to the distribution terminal.
2. Climb pole, open terminal enclosure and note color code of the pair in the distribution cable to which the drop wire is attached.
3. Visually trace distribution cable to the branch feeder terminal and look for suitable place to hide monitoring station.

4. Climb pole, open terminal enclosure and note color code of the binder group containing the pair of interest. Also note if the color code of the pair of interest has changed.

5. Visually trace branch feeder cable to the main feeder cable terminal and look for suitable place to hide monitoring station.

6. Climb pole, open terminal enclosure and note color code of binder group containing the pair of interest. Also note if the color code of the pair of interest has changed.

7. Visually trace main feeder cable to suitable place for hiding monitoring station and look for nearest appearance (assume a terminal enclosure). (Note: terminal enclosure was chosen rather than penetrating cable at a closer point because terminal enclosure is not pressurized but cable is.)

8. Open terminal enclosure and attach own wire-pair to same binding posts to which wire-pair of interest is attached.

9. If the interceptor wishes to check to see if he has the correct pair, he can remove the subscriber side of the pair of interest and attach a test set with ring generator and talk battery to subscriber pair and ring subscriber's telephone. After verification, he re-establishes the normal connection and removes the test set.

10. Run own pair to a high impedance amplifier (battery powered) which he mounts on same or adjacent pole. Run a wire-pair along route to a pole from which the pair can be run into the wooded area with little likelihood of being discovered.

11. Attach monitoring equipment.

2.3 Monitoring Equipment and Procedure

The monitoring equipment could consist of a set of headphones, a signaling decoder and a tape recorder. The first item needs no power. The latter two would be battery powered. Two basic operational procedures are visualized: attended operation and unattended operation.

2.3.1 Attended Operation

The interceptor need be on site only between 6 PM and 11 PM, Monday through Friday. The interceptor would use the headphones to listen to conversations. The signaling decoder could be used to

alert him to an off-hook condition so that he need not listen when telephone is not being used. It could also be used to display the telephone number of parties being called by the targeted individual. If the interceptor wishes to have a record of the conversation of interest, he can manually start tape recorder when the off-hook condition is detected. The tape could be immediately erased if the conversation was not of interest (in order to save tape). The interceptor could take the monitoring equipment with him when he leaves the site in order to minimize chances of accidental discovery of monitoring site.

2.3.2 Unattended Operation

The interceptor need only be on-site for the initial setup, to change tapes and to replace batteries. The headphones would be useful when he is on-site to check the equipment operation. A timer is added to the equipment to energize the equipment at 6 PM and turn it off at 11 PM. The signaling decoder need recognize only the on-hook/off-hook condition and run the recorder only when an off-hook condition exists. Telephone numbers could be identified when tape is played back. The intercept equipment could be camouflaged (perhaps buried) in order to minimize risk of accidental detection.

3.0 INTERCEPTION OF A BUSINESS'S DATA COMMUNICATION TO A COMPUTER SERVICE

3.1 Situation

The interceptor is interested in the data exchanged between a business and a computer center (e.g., the business might have the computer center handling all their accounting). The business always originates the call to the computer center via a special telephone number (unknown to the interceptor). Data is collected by a mini-computer on the premises of the business and periodically transferred to the computer service. The business can interrogate the computer service for processed information (based on its own input data). Information exchange is coded using the American Standard Code for Information Interchange (ASCII) (code used is unknown to interceptor). The modem used is a Bell 203A data set operating at 2400 bps in the half-duplex mode (unknown to interceptor). This is the only data service used by the business.

There are 20 subscriber loops terminating in a PBX. These are carried in a 25-pair aerial distribution cable which runs a short distance outside the premises of the business to a pole-mounted terminal where it is connected to a buried branch feeder cable consisting of 300 pairs (made up of 8 binder groups). Part of the branch feeder cable is laid in a trench through an easement on the property of a building which can be rented. There are no above ground appearances near the property. All cable is Alpeth and the branch feeder cable is pressurized. None of the appearances of the distribution cable are locked or pressurized.

3.2 Signal Acquisition Strategy

A possible strategy for the interceptor is as follows:

1. Visually trace distribution cable to the branch feeder terminal.

2. Climb pole, open terminal enclosure and note color code of binder group in branch feeder cable carrying the 20 subscriber loops. (It is assumed that all subscriber loops are carried in one 25-pair binder group).

3. Visually trace marked right-of-way of the buried branch feeder cable to the property which can be rented. Rent property.

4. Dig trench from building to branch feeder cable and dig up cable.

5. Install gas pressurization by-pass. (By-pass consists of a tube which is connected to cable clamps at both ends.) Drill two small holes (say 24 inches apart) in cable sheath, being careful not to damage pairs and clamp by-pass to the two holes. Cut through cable sheath at two points between the clamps and remove sheath. Plug both ends using a pressure gun filled with a quick-drying compound.

6. Separate binder groups, identify group of interest (from color code), strip insulation from each wire in the group and splice the 25 pairs to 25 voice band high-input impedance amplifiers. Attach own 25-pair cable to outputs of amplifiers and a 2-conductor power cord to a power supply for the amplifiers.

7. Assuming the interceptor knows the correct special three-digit number to dial, he can check to be sure that he has the correct binder group by attaching a standard test set to a working pair and dialing these three digits followed by the last four digits of the telephone number of the business of interest. This action results in a tone being placed on the line by the central office. The interceptor depresses his switch hook momentarily (he may have to repeatedly depress switch hook) until tone goes away. He hangs up. The central office sends out ringing current on the line. The PBX operator answers either with the company name or interceptor asks if he has reached the XYZ company. He makes an excuse and hangs up. (Note: the latter action must be accomplished quickly because some central offices place a tone on the line after about 20 seconds to a few minutes.)

8. Lay the 25-pair cable and the power cord in the trench and fill in the trench and the hole.

9. Attach monitoring equipment and plug power cord into AC outlet.

3.3 Monitoring Equipment and Procedure

The monitoring equipment might consist of a set of headphones; a 25-input signaling decoder for recognizing on-hook/off-hook and 5 dial pulse decoders which display the numbers being called; a modem; a standard oscilloscope; a data scope; a tape recorder; a printer and an intercept equipment controller (e.g., microprocessor).

The interceptor determines the telephone number of the computer service by briefly listening to each line when it goes off-hook and noting the telephone number from the dial pulse decoder display when he hears the distinctive sound of digital data being transmitted. He then sets the controller to recognize (via the dial pulse decoders) when the particular number of the computer service is being called and to connect the line to a pair of output jacks to which he has attached an oscilloscope. By observing the waveform of the line signal, he will be able to determine the modulation and bit rate being used. (In this case, a vestigal sideband, 2-level amplitude modulated carrier operating at 2400 bps.) If he is familiar with the line signals of standard data sets, he could obtain a 203A equivalent from a manufacturer. On the other hand, the interceptor may have on hand a general purpose demodulator with adjustments for detecting the signal. (Note: Line compensation would not be necessary because the interceptor is close enough to the data transmitter.) If the interceptor is able to identify and obtain the appropriate data set, he can proceed to the next step. If not, he must determine the transmitting modem's operations on the input data stream. (In this case, a scrambler using a 23-bit shift register followed by a Binary-to-Gray code converter.) This can be a lengthy process unless the interceptor is familiar with the various types of scramblers used. (Note: This process puts a premium on the interceptor finding out ahead of time the particular modem being used.) The interceptor could defer this problem to a later time by tape recording the line signal.

In either case, after the line signal has been passed through the proper modem, the interceptor must determine the code being used for communication between the business of interest and the computer service (in this case, ASCII). This may be accomplished for standard codes with the aid of a device known as a data scope.

To recover the information of interest, the interceptor will need a printer which accepts the ASCII code and will determine the format of the data by examination of the ouput of the printer.

4.0 INTERCEPTION OF CONVERSATIONS OVER THE DIRECT DISTANCE DIALING NETWORK BETWEEN TWO SPECIFIC INDIVIDUALS IN DIFFERENT CITIES

4.1 Situation

The interceptor is interested in obtaining information being passed in telephone conversations between individuals located in different cities. The interceptor has been able to acquire the numbers of the telephones most likely to be used in making the calls. By studying materials available through the FCC and by physical surveillance, the interceptor has been able to establish that there are three physical routes linking the two cities (as well as other cities near the routes) and the approximate location of each. The three routes are:

- A TD-2 microwave system carrying 14,800 voice channels,
- A coaxial cable having 8 tubes with 1860 voice channels per tube for a total of 14,880 channels, and
- A pressurized multi-pair cable having 200 wire-pairs with 8 of the wire-pairs carrying 24 voice channels each and the remainder single voice channels.

Unknown to the interceptor is the fact that the high usage trunk group between the sectional center in one city and the regional center in the other consists of 36 two-way trunks. Twenty-four are routed via the radio route and twelve via the coaxial route. No trunks of the preferred high-usage trunk group are routed via the multi-pair cable route.

4.2 Signal Acquisition Strategy

The interceptor chooses to be pragmatic in his approach. He knows that the trunk group between the cities is probably divided among the routes. He also knows the difficulties of penetrating and acquiring signals from coaxial cable systems. He is aware of the high voltage hazards and the monitoring and alarm systems associated with the coaxial cables and its repeater stations. The

interceptor decides he does not need to intercept every call made by the targeted individuals. Therefore he chooses to be satisfied with whatever portion of the calls he can acquire from the radio route and the multi-pair cable and to take all the time necessary to get the information he desires.

The interceptor would then proceed to pinpoint the paths of the two routes selected by searching out repeater huts, repeater manholes, cable markers, microwave towers and other indications of rights-of-way. The basic geography of the radio route could be easily determined from FCC filings which are available to the public (and can be subscribed to at nominal cost). An alternative way of determining the radio path would be to simply observe the azimuthal orientation of the antennas on the central office roof and extrapolate the azimuths radiating from the central office location on a suitable map to their destinations.

The interceptor's next steps are to acquire telephone main stations connected with the exchanges to which the targeted telephones are connected and to recruit accomplices. The interceptor would employ several crews to search out the routes, set up interception stations, find the trunk circuits and target the desired communications.

The general strategy for finding the trunk circuits is to have accomplices place calls between telephones connected to the targeted central office switching machines, place easily identifiable tracer signals on the line such as tones and to scan the trunk circuits at the interception sites until the tracer signals are located. The interception sites would then notify the callers that the tone has been found. The callers and interception site personnel would then repeat the process a number of times through-out the day,

sampling the circuits during times of both high and low usage in order to estimate the portion of the high usage trunk group that is assigned to each of the media routed between the exchanges of interest. The specific acquisition activities for the radio and multi-pair cable routes are described below.

4.2.1 Microwave Radio Signal Acquisition

A possible strategy for intercepting the calls on the radio route is as follows:

(1) Locate the microwave repeater sites for the route of interest either through physical observation or from FCC filings,

(2) Acquire the use of a small farm along the route with sufficient line-of-site access to the radiated energy,

(3) Set up radio interception equipment including a sufficiently large antenna (as described in MTR-7439) in a barn to avoid being observed.

(4) Place call between accomplices and put tracer signals on the circuit.

(5) Scan the microwave channels to find tracer signals,

(6) Telephone accomplice from farm either when tracer is found or no tracer tone can be found (accomplice must have second main station telephone to receive such a call) and have him end call and place a new call with the tracer tone.

(7) Begin monitoring the channels on which tracer signals were found.

(8) Continue search for trunk circuits until the portion of the trunk group carried by the microwave route has been approximately identified.

(9) Terminate use of tracer calls and continue to monitor the circuits for desired information.

(10) Program micro-computer equipped with inband signaling decode device to automatically scan the groups of interest. In the

event either of the two targeted telephones is dialed, the scanning device will either signal the interceptor to listen, or automatically connect a recorder to the conversation.

(11) Recorded conversations can either be analyzed for relevant communications in situ or transported to an information extraction facility.

4.2.2 Multi-Pair Cable Signal Acquisition

A possible strategy for the interceptor is as follows:

(1) Trace cable route between cities by means of process discussed above. Find suitable site along cable path either in an isolated area, or on a rentable property, where the interception station can be concealed.

(2) Dig trench from interception station to cable and dig up cable. Upon finding cable to be pressurized, install a gas pressurization bypass, plug cable, and penetrate sheath as described in the previous example.

(3) Splice in 200 pair cable which connects to high impedance amplifier inputs at the interception station. (If the cable run is longer than 300 feet, the high impedance amplifiers will have to be located at the cable or an intermediate point and powered from the interception station). Bury the splice point and cable trench.

(4) Examine all pairs to determine which pairs carry single voice conversations and which carry multiplex systems. Attach either voice-band monitoring equipment or demultiplexing receivers to the pairs according to the types of system found.

(5) Utilize the tracer signal process discussed above to find desired trunk circuits carried by the cable. For wire-pairs carrying single voice conversations, signal back to the accomplices over the wire that the tracer signal had or had not been detected and a new call should be placed. For circuits carrying multiplexed

channels, telephone the accomplice. (If the interception site is in a remote location, the communication to the accomplice would probably need to be relayed by radio (e.g., CB Radio) to another accomplice having access to a telephone.)

(6) After sufficient testing, the interceptor concludes that none of the trunk circuits of interest are routed on the multi-pair cable and concentrates his efforts on getting the desired information from the microwave system.

4.3 Monitoring Equipment and Procedure

Most of the equipment will be required for monitoring the microwave radio route. In addition to a receiver-demultiplexer (which also is used on multi-pair cable route), a radio receiver and antenna system are required. A moderate amount of knowledge and expertise would be required to analyze the radio path, find and install the interception site, and utilize the interception equipment, but the risk of being discovered is fairly low.

The multi-pair cable route requires special tools to dig up the cable and dig a trench to an interception shelter, as well as the cable to interconnect the penetration point with the shelter. The shelter might be a farm house, van or some form of temporary shelter. Special tools and skills will also be required to penetrate the cable, spoof the gas pressurization system, and strip/splice the individual cable pairs. The multi-pair cable interception equipment, if intentionally minimized, could be the least costly of all. Of course, in this example, the desired signals were not on the multi-pair cable.

CHAPTER 119-WIRE INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

18 § 2510

Definitions

As used in this chapter-

(1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire or oral communication other than-

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means-

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; and

(11) "aggrieved person" means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, § 2 Stat. 112.

18 2511 Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who-

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when-

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: Provided, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) It shall not be unlawful under this chapter for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter, is authorized to intercept a wire or oral communication.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.

(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign

intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 213.

Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who willfully-

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of-

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire or oral communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for-

(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier's business, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate

or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 214.

605. Unauthorized publication or use of communications

Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is broadcast or transmitted by amateurs or others for the use of the general public, or which relates to ships in distress.

As amended June 19, 1968, Pub.L. 90-351, Title III, § 803 § 2 Stat. 223.